UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

MICROSOFT CORPORATION, a Washington corporation, Plaintiff, v. JOHN DOES 1 – 10 using IP address 173.11.224.197 Defendants.	No. 2:16-cv-00276 MICROSOFT'S MOTION FOR EXPEDITED DISCOVERY **Note on Motion Calendar:** February 25, 2016[1]

I. INTRODUCTION & RELIEF REQUESTED

Plaintiff Microsoft Corporation ("Microsoft") respectfully moves the Court for an order granting leave to take discovery prior to the Federal Rule of Civil Procedure 26(f) conference. Specifically, Microsoft seeks leave to serve a Rule 45 subpoena on one or more nonparty Internet Service Providers ("ISPs") to obtain records related to the Internet Protocol ("IP") address listed in the above caption. This subpoena will allow Microsoft to identify the Doe Defendants responsible for making unauthorized copies of its intellectual property, and to serve them with this lawsuit. Without expedited discovery, Microsoft cannot determine the identities of the Doe Defendants, and Microsoft will be left without a means to halt the Doe Defendants' ongoing acts of software piracy and intellectual property infringement.

[1] Because Defendants have not been identified or served, and have not yet appeared, this motion is noted for consideration as a same-day ex parte motion pursuant to Local Civil Rule 7(d)(1).

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

II. BACKGROUND

A. The Global Problem of Software Piracy

Software piracy—the unauthorized and unlawful copying, downloading, and distribution of copyrighted and trademarked computer software—is a massive global threat to the continued viability of the software industry. Compl. [Dkt. No. 1] ¶¶ 8–10. Software developers lose billions of dollars in annual revenue from software piracy. *Id.* ¶ 8. In 2013, the commercial value of pirated software in the United States alone exceeded $9.7 billion. *Id.* But software developers are not the only victims of software piracy. Microsoft's customers are also victims, as they are often deceived by distributors of pirated software who go to great lengths to make the software appear genuine. *Id.* ¶ 10. When this occurs, customers may unwittingly expose themselves to security risks associated with the use of pirated software. *Id.*

Microsoft, a Washington corporation, is a leading global software and technology company. Microsoft develops, distributes, and licenses various types of computer software, including operating system software (such as Microsoft Windows). *Id.* ¶ 11. Microsoft holds registered copyrights in the various different versions of these products and has registered trademarks and service marks associated with the products. *Id.* ¶¶ 12–16. These intellectual property rights are infringed whenever Microsoft software is pirated. *Id.*

B. B. Microsoft's Efforts to Combat Software Piracy

Microsoft has implemented a wide-range of initiatives to protect its customers and combat theft of its intellectual property. One important tool in Microsoft's anti-piracy arsenal is its product activation system, which involves the activation of software through product keys. *Id.* ¶ 25. A Microsoft product key is a 25-character alphanumeric string generated by Microsoft and provided either directly to Microsoft's customers or to Microsoft's original equipment manufacturer ("OEM") partners. *Id.* ¶ 26. Generally, when customers or OEMs install Microsoft software on a device, they must enter the product key. *Id.* Then, as part of the activation process, customers and/or OEMs voluntarily contact Microsoft's activation servers over the Internet and transmit the product keys and other technical information about their

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

device to the servers. *Id.* Because Microsoft software is capable of being installed on an unlimited number of devices, Microsoft uses the product activation process to detect piracy and protect consumers from the risk of non-genuine software. *Id.* ¶ 27.

To support Microsoft's global anti-piracy efforts, Microsoft recently created the Microsoft Cybercrime Center. *Id.* ¶ 31. Among other tools, the Cybercrime Center utilizes investigative methods that leverage state-of-the-art technology to detect software piracy; Microsoft refers to these methods as "cyberforensics." *Id.* Microsoft uses cyberforensics to analyze product key activation data voluntarily provided by users when they activate Microsoft software, including the IP address[2] from which a given product key is activated. *Id.* ¶ 32. Cyberforensics allows Microsoft to analyze billions of activations of Microsoft software and identify activation patterns and characteristics that make it more likely than not that the IP address associated with certain product key activations is one through unauthorized copies of Microsoft software are being activated. Decl. of Brittany Carmichael ("Carmichael Decl.") ¶ 2. These characteristics include software activations with (a) product keys known to have been stolen from Microsoft's supply chain; (b) product keys used more times than is authorized by the applicable software license; (c) product keys used by someone other than the authorized licensee; and (d) product keys activated outside of the region for which they were intended. *Id.* ¶ 3. Microsoft's cyberforensics routinely identify IP addresses engaging in numerous product key activations that satisfy at least one (and sometimes more) of these criteria. *Id.*

C. Defendants' Infringing Conduct

Microsoft's cyberforensics have identified thousands of product key activations originating from IP address 173.11.224.197 (the "Infringing IP Address"). *Id.* ¶ 4. According to publicly available data, the Infringing IP Address is presently assigned to Comcast Cable Communications ("Comcast"), an ISP. *Id.* Microsoft believes that Comcast has, in turn,

[2] The IP address is a numerical identifier used to uniquely identify an internet-capable device when the device is connected to the Internet, and is ordinarily assigned to an internet user (whether an individual or an entity) by the user's ISP. *Id.*

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

assigned possession and control of the Infringing IP address to either the Doe Defendants or to a downstream ISP who has assigned it to the Doe Defendants. *Id.*

For an unknown period of time—but for at least the past three years—the Infringing IP Address has been used to activate thousands of Microsoft product keys. *Id.* ¶ 5. Almost all of these activations have involved voluntary contact and communication between one or more of the Doe Defendants and certain Microsoft activation servers, the vast majority of which are physically located in this judicial district. *Id.* These activations have characteristics that demonstrate that one or more of the Doe Defendants are using the Infringing IP Address to activate unauthorized copies of Microsoft's software. *Id.* The Infringing IP Address has been used to activate copies of Windows 8, Windows 7, Office 2010, Windows Server 2012, and Windows Server 2008 with product keys that have some or all of the following characteristics: (a) product keys known to have been stolen from Microsoft's supply chain; (b) product keys used more times than is authorized by the applicable software license; (c) product keys used by someone other than the authorized licensee; and (d) product keys activated outside of the region for which they were intended. Microsoft believes these activations constitute the unauthorized copying, distribution, and use of Microsoft software. *Id.* ¶ 6. Microsoft believes these activations constitute the unauthorized copying, distribution, and use of Microsoft software, in violation of Microsoft's software licenses and intellectual property rights. *Id.*

Despite reasonable efforts, including various investigative techniques, Microsoft has been unable to positively identify the Doe Defendants. *Id.* ¶ 7. At present, the best information Microsoft has for identifying the Doe Defendants is the Infringing IP Address and the dates and times the Doe Defendants used the Infringing IP Address to activate product keys in a manner consistent with software piracy. *Id.* The only reliable way Microsoft can determine the Doe Defendants' actual identities is by obtaining the subscriber information associated with the Infringing IP Address from the ISP who assigned the Infringing IP Address to the Doe Defendants. *Id.* ¶ 8.

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

Microsoft believes Comcast has access to the subscriber information associated with the Infringing IP Address from records kept in the regular course of its business. *Id.* ¶ 9. However, Microsoft also understands that Comcast will not provide subscriber information to a third party without the consent of the subscriber or a court order. *Id.* Microsoft therefore seeks leave to serve a Rule 45 subpoena on Comcast (and, if necessary, on downstream ISPs to whom Comcast may have assigned the Infringing IP Address), for the sole purpose of determining the identities of the Doe Defendants.

III. ARGUMENT

A. Legal Standard

Federal Rule of Civil Procedure 26 provides that a party "may not seek discovery from any source before the parties have conferred as required by Rule 26(f), except . . . when authorized . . . by court order." Fed. R. Civ. P. 26(d)(1). Although the Ninth Circuit has not directly defined the standard for allowing expedited discovery, "courts in this jurisdiction require that the moving party demonstrate that 'good cause' exists to deviate from the standard pretrial schedule." *Music Grp. Macao Commercial Offshore Ltd. v. John Does I-IX*, 2014 WL 11010724, at *1 (W.D. Wash. July 18, 2014) (Martinez, J.). Judges in this district routinely apply the "good cause" standard in granting motions for expedited discovery. *See id.*; *Fluke Elecs. Corp. v. CorDEX Instruments, Inc.*, 2013 WL 566949, at *10 (W.D. Wash. 2013) (Robart, J.); *Microsoft Corp. v. Mai*, 2009 WL 1393750, at *5 (W.D. Wash. 2009) (Jones, J.); *Renaud v. Gillick*, 2007 WL 98465, at *2 (W.D. Wash. Jan. 8, 2007) (Lasnik, J.).

"Good cause exists 'where the need for expedited discovery, in consideration of the administration of justice, outweighs the prejudice to the responding party.'" *Microsoft Corp.*, 2009 WL 1393750, at *5 (quoting *Semitool, Inc. v. Tokyo Electron Am., Inc.*, 208 F.R.D. 273, 276 (N.D. Cal. 2002)). The relevant factors in assessing good cause are the requesting party's diligence, its intent in seeking the requested information, and whether the opposing party will be prejudiced if the Court grants the motion. *See Renaud*, 2007 WL 98465, at *3; *Music Grp.*,

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

2014 11010724, at *1. Courts routinely allow early discovery where it will "substantially contribute to moving th[e] case forward" and is "narrowly tailored" for that purpose. *Semitool*, 208 F.R.D. at 277; *Music Grp.*, 2014 WL 11010724, at *2. "[C]ourts have recognized that good cause is frequently found in cases involving claims of infringement and unfair competition." *Semitool*, 208 F.R.D. at 276.

B. Good Cause Exists for Expedited Discovery.

1. Expedited Discovery Is Warranted Because Microsoft Must Identify the Doe Defendants to Properly Serve Them.

"[W]here the identity of alleged defendants will not be known prior to the filing of a complaint . . . the plaintiff should be given an opportunity through discovery to identify the unknown defendants, unless it is clear that discovery would not uncover the identities, or that the complaint would be dismissed on other grounds." *Gillespie v. Civiletti*, 629 F.2d 637, 642 (9th Cir. 1980). The Ninth Circuit has repeatedly urged district courts to allow plaintiffs to conduct discovery when necessary to identify unknown defendants. *See id.; Wakefield v. Thompson*, 177 F.3d 1160, 1163 (9th Cir. 1999); *see also Young v. Transp. Deputy Sheriff I*, 340 Fed. Appx. 368, 369 (9th Cir. 2009) (vacating judgment and remanding for district court to allow plaintiff the opportunity to discover the identity of two unknown deputy sheriff defendants); *Cottrell v. Unknown Corr. Officers*, 1–10, 230 F.3d 1366 (9th Cir. 2000) (district court erred in dismissing action with no named defendants because expedited discovery could have allowed plaintiff to identify unknown correctional officers).

Expedited discovery is particularly appropriate when plaintiff does not know the identity of the defendants at the time the complaint is filed but can learn their identity through early discovery. *See, e.g., Music Grp.*, 2014 WL 11010724, at *1 ("Courts routinely permit early discovery for the limited purpose of identifying 'Doe' defendants on whom process could not otherwise be served."). If plaintiff does not know the identities of the defendants, it makes no sense to defer discovery until after the Rule 26(f) conference because "[o]bviously, a plaintiff cannot have a [Rule 26(f)] conference with an anonymous defendant." *UMG*

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

Recordings, Inc. v. Doe, 2008 WL 4104207, at *2 (N.D. Cal. 2008). "It follows that the discovery [plaintiffs] are entitled to conduct to identify the defendant[s] must take place before the [Rule 26(f)] conference because such information will permit the [plaintiff] to identify [the] Doe [defendants] and serve [them], permitting this case to go forward." *Id*.

Here, Microsoft does not currently know the identities of the Doe Defendants, but reasonably believes it can determine their identities through limited expedited discovery. Carmichael Decl. ¶¶ 7 & 10. Because all of the defendants in this lawsuit are presently unknown, Microsoft cannot hold a Rule 26(f) conference with anonymous defendants. Absent an order permitting expedited discovery, this case cannot move forward.

2. The Relevant Factors All Support Expedited Discovery.

The Court considers three factors to assess the propriety of expedited discovery: (1) Microsoft's diligence, (2) its intent in seeking the information, and (3) prejudice to Defendants. *See Renaud*, 2007 WL 98465, at *3; *Music Grp.*, 2014 WL 1101072, at *1. Each factor supports granting Microsoft's motion:

Microsoft's Diligence. Microsoft has been diligent in attempting to uncover the identities of the Doe Defendants. Carmichael Decl. ¶ 7. After Microsoft identified and verified the Infringing IP Address as the source of product key activations consistent with software piracy, Microsoft utilized publicly available data to determine the Infringing IP Address is under the control of an ISP—namely, Comcast. However, Microsoft could not (and cannot) determine the identity of the subscriber(s) utilizing the Infringing IP Address without a court order. *Id*. ¶¶ 8–9; see also 47 U.S.C. § 551(c) (prohibiting a cable operator from "disclos[ing] personally identifiable information concerning any subscriber without the prior written or electronic consent of the subscriber . . . [or] pursuant to a court order"). Accordingly, this factor supports granting Microsoft leave to conduct expedited discovery.

Microsoft's Intent. Microsoft seeks information identifying the subscribers associated with the Infringing IP Address for the sole purpose of determining the identities of the Doe

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

Defendants and serving them with this lawsuit. An order granting Microsoft leave to obtain this information is the only reliable way Microsoft can determine the identities of the Doe Defendants. Carmichael Decl. ¶ 8. Because Microsoft's intent is to "advance the litigation and save judicial resources," *Renaud*, 2007 WL 98465, at *3, this factor supports granting Microsoft leave to conduct expedited discovery.

Prejudice to Defendants. Defendants will suffer no cognizable prejudice if Microsoft is granted leave to conduct expedited discovery. Microsoft's request for expedited discovery is narrowly tailored to include only the information necessary to identify the subscriber(s) using the Infringing IP Address at the time of alleged infringement. Further, the Doe Defendants have no legitimate expectation of privacy in the subscriber information they provided to their ISP. *See, e.g.*, *Guest v. Leis*, 255 F.3d 325, 336 (6th Cir. 2001) ("[C]omputer users do not have a legitimate expectation of privacy in their subscriber information because they have conveyed it to another person—the system operator."); *United States v. Christie*, 624 F.3d 558, 573 (3rd Cir. 2010) ("Federal courts have uniformly held that 'subscriber information provided to an internet provider is not protected by the Fourth Amendment's privacy expectation' because it is voluntarily conveyed to third parties."); *Worldwide Film Entm't, LLC v. Does 1-749*, 2010 WL 1946926, at *2 (D.D.C. 2010) (denying motion to quash subpoena seeking ISP subscriber information because "subscribers do not have a claim of confidentiality in their subscriber information"). Finally, the requested discovery is directed at a non-party ISP, not the Doe Defendants. Granting "third party document requests will not impose a significant burden on [D]efendants," *Renaud*, 2007 WL 98465, at *3, which further shows the Doe Defendants will suffer no cognizable prejudice if the Court grants Microsoft's motion.

IV. CONCLUSION

For the foregoing reasons, Microsoft respectfully asks the Court to grant Microsoft leave to conduct expedited discovery prior to the Rule 26(f) conference so Microsoft can uncover the identities of the Doe Defendants responsible for stealing its intellectual property,

Davis Wright Tremaine LLP
LAW OFFICES
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
206.622.3150 main · 206.757.7700 fax

and serve them with this lawsuit. Specifically, Microsoft seeks leave to serve a Rule 45 subpoena on Comcast to obtain subscriber information associated with the Infringing IP Address at the time of the alleged acts of infringement. If Comcast identifies a downstream ISP (rather than the Doe Defendants) as the entity to whom it has assigned use and control of the Infringing IP Address, Microsoft further requests leave to serve a Rule 45 subpoena on that downstream ISP (and any additional downstream ISPs) until the identity of the Doe Defendants can be determined. A proposed order to this effect is attached.

DATED this 25th day of February, 2016.

DAVIS WRIGHT TREMAINE LLP
Attorneys for Plaintiff Microsoft Corp.

By *s/ Brooke Howlett*
Brooke Howlett, WSBA #47899
1201 Third Avenue, Suite 2200
Seattle, WA 98101-3045
Telephone: (206)757-8187
Fax: (206)757-7187
E-mail: brookehowlett@dwt.com